AMENDMENTS TO THE CLAIMS

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 were pending at the time of the Action.

Claims 1, 10, 12, 16, 24, 26, 31, 38, 40, 49, and 58 are amended.

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 remain pending.

1. (Currently Amended) A method for constraining a scope of delegation by a client to a server, comprising:

identifying a target service to which access is sought on behalf of a client;

causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third-party, wherein the server provides the trusted third-party with a credential authenticating the server, information about the target service, and a service credential previously provided by the client to the server; and

causing the trusted third-party to provide the server with a new service credential granted in the name of the client rather than the server such that the new service credential authorizes the server to access the target service on behalf of the client while withholding a client's authentication credentials from the server, wherein the new service credential granted in the name of the client is constrained to a scope specified by the service credential previously provided by the client to the server.

2. (Original) The method as recited in Claim 1, wherein the trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

3. (Canceled).

4. (Previously Presented) The method as recited in Claim 1, wherein the new service credential is configured for use by the server and the target service to which access is sought.

5. (Previously Presented) The method as recited in Claim 1, wherein the credential authenticating the server is a ticket that includes a ticket granting ticket associated with the server.

6. (Original) The method as recited in Claim 1, further comprising:

causing the trusted third-party to verify that the client has authorized delegation.

7. (Original) The method as recited in Claim 6, wherein:

the trusted third-party includes a key distribution center (KDC); and

causing the trusted third-party to verify that the client has authorized delegation includes verifying the status of a restriction placed on the ticket originating from the client.

8. (Original) The method as recited in Claim 1, further comprising:

causing the trusted-third-party to selectively determine if the client is allowed to participate in delegation either based on information selected from a group comprising an identity of the client, a group affiliation associated with the client.

9. (Original) The method as recited in Claim 1, wherein the server is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service to which access is sought.

10. (Currently Amended) The method as recited in Claim 1, wherein:

the trusted third-party includes a key distribution center (KDC);

the KDC provides the client's authentication credentials as a ticket-granting-ticket associated with the client to the client; and

the client does not provide the ticket granting ticket to the server.

11. (Original) The method as recited in Claim 1, wherein:

the trusted third-party includes a key distribution center (KDC); and

the server requests the new credential in a ticket granting service request message that includes a service ticket provided by the client to the server.

12. (Currently Amended) A method for constraining the scope of authentication credential delegation by a client to a server, comprising:

identifying a target service to which access is sought on behalf of a client; and

causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third party, wherein the server provides the trusted third party with a service credential authenticating the server, information about the target service, and a service credential previously provided by the client for the service, and wherein the service credential previously provided by the client includes implementation-specific identity information constraining a scope of access delegated to the server; and

causing the trusted third-party to provide the server with a new service credential ~~granted in the name of the client rather than the server~~ such that the new service credential authorizes the server to access the target service within the scope of access specified in the implementation-specific identity information.

13. (Original) The method as recited in Claim 12, wherein the implementation-specific identity information includes information selected from a group comprising privilege attribute certificate (PAC) information, security identifier information, Unix identifier information, Passport identifier information, certificate information.

14. (Original) The method as recited in Claim 13, wherein the PAC information includes compound identity information.

15. (Original) The method as recited in Claim 13, wherein the PAC information includes access control restrictions for use as delegation constraints.

16. (Currently Amended) A computer-readable medium having computer-executable instructions for performing tasks for constraining a scope of delegation by a client to a server, comprising:

in a server, determining a target service to which access is sought on behalf of a client coupled to the server;

requesting a new service credential from a trusted third-party by providing the trusted third-party with a credential authenticating the server, information about the target service, and a service credential associated with the client and the requesting server such that issuance of the new service credential authorizes the server to access the service on behalf of the client while within a scope of delegation authorized by the client.

17. (Original) The computer-readable medium as recited in Claim 16, wherein the trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

18. (Canceled).

19. (Previously Presented) The computer-readable medium as recited in Claim 16, wherein the service credential is configured for use by the server and the target service.

20. (Previously Presented) The computer-readable medium as recited in Claim 16, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.

21. (Original) The computer-readable medium as recited in Claim 16, further comprising:

causing the trusted third-party to verify that the client has authorized delegation.

22. (Original) The computer-readable medium as recited in Claim 21, wherein:

the trusted third-party includes a key distribution center (KDC); and

causing the trusted third-party to verify that the client has authorized delegation includes verifying the status of a forwardable flag value as set by the client.

23. (Original) The computer-readable medium as recited in Claim 16, wherein the server is a front-end server with respect to a back-end server coupled to the front-end server, and wherein the back-end server is configured to provide the target service.

24. (Currently Amended) The computer-readable medium as recited in Claim 16, wherein:

the trusted third-party includes a key distribution center (KDC);

the KDC provides to the client authentication credentials of the client as a ticket-granting-ticket associated with the client ~~to the client~~; and

the client does not provide the ticket granting ticket to the server.

25. (Original) The computer-readable medium as recited in Claim 16, wherein:

the trusted third-party includes a key distribution center (KDC); and

the requesting server requests the new service credential in a ticket granting service request message that includes a service ticket provided by the client to the server.

26. (Currently Amended) A system comprising:

a credential granting mechanism configured to receive a request for a new service credential from a server and in response generate the new service credential granted in the name of a client rather than the server if delegation is allowable, and wherein the request includes:

a credential authenticating the requesting server,

identifying information about a target service to which access is sought on behalf of the client coupled to the server, and

a service credential that was previously granted to the client for use with the server and presenting a forwardable delegation flag indicating the client has authorized the delegation within a scope delegated by the client.

27. (Original) The system as recited in Claim 26, wherein the credential granting mechanism is provided by a trusted third party and includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

28. (Canceled).

29. (Previously Presented) The system as recited in Claim 26, wherein the service credential is configured for use by the server and the target service.

30. (Previously Presented) The system as recited in Claim 26, wherein the credential authenticating the server includes a ticket granting ticket associated with the server, and which was previously granted by the credential granting mechanism.

31. (Currently Amended) A system for constraining the scope of delegation by a client to a server, comprising:

a server configured to generate a request for a new service credential in the name of a client rather than the server from a trusted third-party, the new service credential being associated with a client and a target service, the request comprising:

a credential authenticating the server,

information about the target service, and

a service credential associated with the client and the server wherein the server is constrained to access the target service within a scope specified by the client.

32. (Original) The system as recited in Claim 31, wherein the trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

33. (Original) The system as recited in Claim 31, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.

34. (Original) The system as recited in Claim 31, wherein the server is a front-end server with respect to the service.

35. (Original) The system as recited in Claim 31, wherein the server requests the new service credential in a ticket granting service request message that includes the service ticket associated with the client and the server.

36. (Withdrawn) A computer-readable medium having stored thereon a data structure, comprising:

a credential authenticating a first server,

information identifying a second server, and

a service credential associated with a client and the first server.

37. (Withdrawn) The computer-readable medium as recited in Claim 36, wherein the credential authenticating the first server includes a ticket-granting-ticket (TGT) and the service credential includes a service ticket.

38. (Currently Amended) A method comprising:

separately authenticating a server and a client;

providing the server with a server ticket granting ticket;

providing the client with a client ticket granting ticket and a service ticket for use with the server;

providing the server with a new service ticket in an identity of the client rather than an identity of the server for use by the server ~~for use~~ with a new service while withholding from the server ~~without requiring the server to have~~ access to the client ticket granting ticket thereby constraining delegation of the client ticket granting ticket.

39. (Original) The method as recited in Claim 38, further comprising:

causing the server to request the new service ticket on behalf of the client by forwarding the server ticket granting ticket, information identifying the new service, and the service ticket to a trusted third party.

40. (Currently Amended) A method for constraining a scope of delegation by a client to a server, comprising:

identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;

causing a server that is operatively coupled to the target service and the client to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication ~~protocol~~ method; and

causing the server to request from the second authentication method trusted third-party, a new service credential in an identity of the client rather than an identity of the server, for use by the server and the target service, ~~from the second authentication method trusted third-party,~~ wherein the server provides the trusted third-party with a credential authenticating the server to access the target service within a scope constrained by the client, information about the target service, and the service credential to itself.

41. (Original) The method as recited in Claim 40, wherein the second authentication method trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

42. (Canceled).

43. (Previously Presented) The method as recited in Claim 40, wherein the service credential is configured for use by the server and the target service to which access is sought.

44. (Previously Presented) The method as recited in Claim 40, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.

45. (Original) The method as recited in Claim 40, further comprising:

upon receiving a request for the new service credential from the server, causing the second authentication method trusted third-party to verify that the client has authorized delegation.

46. (Original) The method as recited in Claim 40, wherein the server is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service.

47. (Original) The method as recited in Claim 40, wherein the first authentication method is selected from a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

48. (Original) The method as recited in Claim 40, wherein the second authentication method includes a Kerberos authentication protocol.

49. (Currently Amended) A computer-readable medium having computer-executable instructions for performing tasks for constraining a scope of delegation by a client to a server, comprising:

identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;

causing a server that is operatively coupled to the target service and the client to request a service ticket to itself from a second authentication method trusted third-party by identifying the client and the first authentication method ~~protocol~~; and

causing the server to request a new service ticket in an identity of the client rather than an identity of the server, for use by the server and the identified service, from the second authentication method trusted third-party, wherein the server provides the trusted third-party with a ticket authenticating the server to act within a scope of delegation permitted by the client, information about the target service, and the service ticket to itself.

50. (Original) The computer-readable medium as recited in Claim 49, wherein the second authentication method trusted third-party includes a key distribution center (KDC).

51. (Canceled).

52. (Previously Presented) The computer-readable medium as recited in Claim 49, wherein the service ticket is configured for use by the server and the target service.

53. (Previously Presented) The computer-readable medium as recited in Claim 49, wherein the ticket authenticating the server includes a ticket granting ticket associated with the server.

54. (Original) The computer-readable medium as recited in Claim 49, further comprising:

upon receiving a request for the new service ticket from the server, causing the second authentication method trusted third-party to verify that the client has authorized delegation.

55. (Original) The computer-readable medium as recited in Claim 49, wherein the server is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service.

56. (Original) The computer-readable medium as recited in Claim 49, wherein the first authentication method is selected from a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

57. (Original) The computer-readable medium as recited in Claim 49, wherein the second authentication method includes a Kerberos authentication protocol.

58. (Currently Amended) A system for constraining a scope of delegation by a client to a server, comprising:

a server configurable to:

identify a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method,

request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication method, and

subsequently request a new service credential, for use by the server and the target service, from the second authentication method trusted third-party,

wherein the server provides the second authentication method trusted third-party with a credential authenticating the server, information about the target service, and the service credential to itself in an identity of the client rather than the server such that a scope of delegation authorized by the client constrains access by the server to the target service as authorized by the client.

59. (Canceled).

60. (Previously Presented) The system as recited in Claim 58, wherein the new service credential is configured for use by the server and the target service.

61. (Previously Presented) The system as recited in Claim 58, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.